JOURNAL OF COMBINATORIAL THEORY, Series A **75**, 341–352 (1996)
ARTICLE NO. 0082

Maximal Subgroups of Symmetric Groups

MARTIN W. LIEBECK

Department of Mathematics, Imperial College, London SW7 2BZ, England

AND

ANER SHALEV

Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel

Communicated by László Babai

Received December 1995

We show that S_n has at most $n^{6/11+o(1)}$ conjugacy classes of primitive maximal subgroups. This improves an $n^{c\log^3 n}$ bound given by Babai. We conclude that the number of conjugacy classes of maximal subgroups of S_n is of the form $(\frac{1}{2}+o(1))n$. It also follows that, for large n, S_n has less than $n!$ maximal subgroups. This confirms a special case of a conjecture of Wall. Improving a recent result from [MSh], we also show that any finite almost simple group has at most $n^{17/11+o(1)}$ maximal subgroups of index n.

1. INTRODUCTION

The main purpose of this paper is to show that the symmetric group S_n has very few maximal subgroups. It is clear that S_n has $[n/2]$ conjugacy classes of intransitive maximal subgroups (of type $S_k \times S_{n-k}$), and it follows from our main result that the number of conjugacy classes of transitive maximal subgroups is much smaller; it is bounded above by $n^{6/11+o(1)}$ (see Corollary 4.5 below). We can therefore say that, in a sense, almost all maximal subgroups of S_n are the obvious intransitive ones.

Note that the number of conjugacy classes of transitive maximal subgroups of S_n which are imprimitive is $d(n)-2$, where $d(n)$ is the number of divisors of n. It is well known that $d(n)=n^{o(1)}$ (see, for instance, [HW, Theorem 315]). It therefore remains to enumerate primitive maximal subgroups. In 1989 Babai showed that S_n has at most $n^{c\log^3 n}$ conjugacy classes of primitive maximal subgroups [B, Lemma 2.5]. His result, as well as ours, relies on the Classification of Finite Simple Groups. In fact, using the O'Nan-Scott Theorem (see [KL, p. 6]), it is easy to derive good bounds

0097-3165/96 $18.00

on the number of classes of primitive maximal subgroups of S_n which are not almost simple, and so it remains to enumerate almost simple primitive maximal subgroups of S_n. At this stage we ignore the maximality condition, and bound the number of conjugacy classes of almost simple primitive subgroups of S_n (including the non-maximal ones). In other words, given n, we bound the number of pairs (G, M) such that G is an almost simple group, and M is an index n maximal subgroup of G (up to conjugacy in G). This is where the Classification, and the information on the subgroup structure of finite simple groups, is invoked.

Our enumeration of these pairs (G, M) is carried out in two natural steps. First, we bound the number of conjugacy classes of index n maximal subgroups M which a given almost simple group G can have; then we bound the number of possibilities for G (up to isomorphism).

The second step amounts to enumerating isomorphism classes of primitive almost simple subgroups of S_n; we show that the number of such isomorphism classes is at most $(\log n)^{9+o(1)}$ (see Proposition 4.2), hence in particular is of the form $n^{o(1)}$. The main tool in the proof is the derivation of polynomial expressions for the indices of maximal subgroups of almost simple groups of Lie type (see Theorem 3.1, which may be of some independent interest).

In the first step we estimate the number $m_n(G)$ of maximal subgroups of index n in an almost simple group G, using recent results from [LSe1], [LSe2], [LiSh2] and [LiSh3] as our main tools. Note that it has recently been shown in [MSh] that $m_n(G) \leqslant n^{1+7/8+o(1)}$ for all almost simple groups G. Here we improve this result, showing that $m_n(G) \leqslant n^{1+6/11+o(1)}$. The core of our proof is the enumeration of 'unknown' almost simple maximal subgroups M of G, where G is an exceptional group of Lie type. Writing $M = N_G(M_0)$ where $M_0 < G$ is simple, we have to count the possibilities for M_0. To do this we use the fact, established in [LiSh3] (see also [MSW]) that a randomly chosen involution and a randomly chosen additional element generate any finite simple group M_0 with probability $\geqslant \varepsilon$, where ε is some absolute positive constant. Using the existence of such a generating pair, and counting multiplicities, it follows that the number of subgroups of G which are isomorphic to M_0 is at most $\varepsilon^{-1}(i_2(G)\,|G|)/(i_2(M_0)\,|M_0|)$, where $i_2(H)$ denotes the number of involutions in a group H. Now, the possibilities for M_0 are described in [LSe1], [LSe2], while the estimates for $i_2(G)$, $i_2(M_0)$ can be found in [LiSh2]. Applying these, we derive the above mentioned bound on $m_n(G)$.

At this stage it follows that an almost simple group has at most $n^{6/11+o(1)}$ conjugacy classes of index n maximal subgroups (since each conjugacy class consists of n subgroups). In other words, each isomorphism type of primitive almost simple subgroups of S_n splits into at most $n^{6/11+o(1)}$ S_n-conjugacy classes. Combining this with the results of the second step we

conclude that S_n has $n^{o(1)}.n^{6/11+o(1)} = n^{6/11+o(1)}$ almost simple primitive subgroups up to conjugacy.

We note that the number of conjugacy classes of primitive (not necessarily maximal) subgroups of S_n is considerably larger. It can be shown that this number is bounded above by $n^{c \log n}$ for all n, and bounded below by $n^{c' \log n/\log\log n}$ for infinitely many values of n [PSh2]. See also [P], [PSh1] for related results, and for applications of estimates of this type to subgroup growth of infinite groups.

Our results concerning the number of conjugacy classes of maximal subgroups of S_n can be used to answer a particular case of an old question of G.E. Wall. In his 1961 paper [Wa], Wall showed that the number of maximal subgroups of a finite soluble group is less than the group order, and suggested that a similar result might hold for finite groups in general. We show that this is the case if G is a symmetric (or alternating) group of large degree. We are grateful to Laci Pyber for drawing our attention to Wall's question.

We conclude the introduction by posing some conjectures. The first is a sharper version of our main result.

Conjecture 1. S_n has $n^{o(1)}$ conjugacy classes of primitive maximal subgroups.

The results of this paper reduce this conjecture to the assertion that $m_n(G) \leqslant n^{1+o(1)}$ *for all almost simple groups* G, as conjectured in [MSh]. While this assertion holds for classical and alternating groups, it is still very much open for the (large rank) exceptional groups of Lie type.

Conjecture 2. There exists an absolute constant c such that S_n has at most c isomorphism classes of simple primitive subgroups.

This conjecture has a strong number-theoretic flavour. One is required to show that, given n, the number of simple groups which have a maximal subgroup of index n is bounded *independently of* n. Some particular cases of this seem interesting in their own right. For instance, can a given number n be expressed as a binomial coefficient $\binom{m}{k}$ in more than $O(1)$ ways?

Our notation is rather standard and follows that of [LiSh1], [LiSh2]. All groups considered will be finite. By a simple group we mean a non-abelian simple group. An almost simple group is a group lying between a simple group and its automorphism group. The notation $A_n^\varepsilon(q)$ $(\varepsilon = \pm)$ denotes $A_n(q)$ if $\varepsilon = +$ and ${}^2A_n(q)$ if $\varepsilon = -$; similarly for types D_n^ε, B_2^ε, G_2^ε, F_4^ε and E_6^ε. For two expressions f, g we write $f \sim g$ if the ratio f/g is bounded between two positive constants (i.e. $f = \Omega(g)$). Throughout this paper c, c', c_i, ... denote absolute constants, and p denotes a prime number. The number of divisors of an integer n is denoted by $d(n)$. The number of

maximal subgroups of index n in G is denoted by $m_n(G)$. We denote the number of involutions in a group G by $i_2(G)$. Finally, $\log x$ stands for $\log_2 x$.

2. Counting Maximal Subgroups

In this section we use some recent results from [LSe1, LSe2] and [LiSh2, LiSh3] in order to enumerate maximal subgroups of given index in almost simple groups. Our main conclusion (Theorem 2.4) improves [MSh, Theorem 1 and Lemmas 8-10], which state that, if G is almost simple, then $m_n(G) = n^{1+o(1)}$ provided $\mathrm{soc}(G)$ is not of type F_4, E_6^ε, E_7 or E_8, and that in the latter cases we have $m_n(G) \leqslant n^{\alpha+o(1)}$ where $\alpha = 15/8$, $9/5$, $173/103$, $5/3$, respectively.

Theorem 2.1. *Let G be a finite almost simple group with socle G_0 which is of type F_4, E_6^ε, E_7, E_8 over $\mathbb{F}_q$, where $q = p^a$, and let M be a maximal subgroup of G not containing G_0. If M is almost simple let M_0 denote its socle. Then one of the following holds*:

(i) *M is a known subgroup, belonging to one of boundedly many conjugacy classes*;

(ii) *M is the centralizer of a field automorphism of G_0 (there are at most $c.d(a)$ classes of such automorphisms)*;

(iii) *M is almost simple of bounded order*;

(iv) *$G_0 \cong F_4(q)$, $p \leqslant 3$ and $M_0 \cong A_1(q)$, $A_2^\varepsilon(q)$, $B_2^\varepsilon(q)$ or $G_2(q)$*;

(v) *$G_0 \cong E_6^\varepsilon(q)$, $p \leqslant 5$ and $M_0 \cong A_1(q)$, $A_2^\delta(q)$, $B_2^\delta(q)$, $G_2^\delta(q)$, or $B_3(q)$*;

(vi) *$G_0 \cong E_7(q)$, $p \leqslant 7$ and $M_0 \cong A_1(q)$, $A_2^\varepsilon(q)$, $B_2^\varepsilon(q)$, $G_2^\varepsilon(q)$, or $B_3(q)$*;

(vii) *$G_0 \cong E_8$, $p \leqslant 7$ and $M_0 \cong A_1(q)$, $A_2^\varepsilon(q)$, $B_2^\varepsilon(q)$, $G_2^\varepsilon(q)$, $B_3(q)$, $A_3^\varepsilon(q)$, $C_3(q)$ or $B_4(q)$.*

Proof. Assume first that M is not almost simple. Such maximal subgroups are determined by [LSe1, Theorem 2]. In conclusions (a), (b), (d) and (e) of this result M falls into boundedly many conjugacy classes, as in (i). In conclusion (c), M is the centralizer of a field, a graph, or a graph-field automorphism of G_0; there are boundedly many classes of graph and graph-field automorphisms (see [GL, 7.2]), so (i) or (ii) holds.

Now assume M is almost simple, and is not the centralizer of a field automorphism. Write $G_0 = O^{p'}(\bar{G}_\sigma)$, where σ is a Frobenius morphism of a simple algebraic group $\bar{G}$ over $\bar{\mathbb{F}}_p$ of the same type as G_0. According to [LSe2, Corollary 5], there is a constant c such that either $|M| < c$, or $M = N_G(\bar{X}_\sigma)$ for some maximal closed connected $M\langle\sigma\rangle$-invariant subgroup $\bar{X}$ of G. The first case gives (iii), so suppose the latter holds.

If $\bar{X}$ is not simple, then it is determined by [LSe1, Theorem 1]; and each of the conclusions (a)–(d) of this result give rise to boundedly many classes of subgroups $N(\bar{X}_\sigma)$ in G, which we subsume into (i). If $\bar{X}$ is simple and $p > N(\bar{X}, \bar{G})$ (notation from [LSe1, Table I]), then again $\bar{X}$ is given by [LSe1, Theorem 1], again giving boundedly many classes in G. Finally, if $\bar{X}$ is simple and $p \leqslant N(\bar{X}, \bar{G})$, then $\bar{X}_\sigma$ is a group over $\mathbb{F}_q$, and one of conclusions (iv)–(vii) holds. ▮

We can now estimate the number of *isomorphism types* of maximal subgroups in exceptional groups of Lie type.

COROLLARY 2.2. *If G is an almost simple exceptional group of Lie type over $\mathbb{F}_q$, where $q = p^a$, then G has at most $c.d(a)$ isomorphism types of maximal subgroups.*

Proof. This follows from 2.1 for types F_4, E_6^ε, E_7, E_8 (note that for M_0 as in (iv)–(vii) of 2.1, there are at most $c.d(a)$ isomorphism types of subgroups M with socle M_0, since $\mathrm{Out}(M_0)$ has at most $c.d(a)$ subgroups). Finally, the result follows for the other types from the known lists of maximal subgroups in [Co, Kl1, Kl2, Ma, Su]. ▮

PROPOSITION 2.3. *Let G be almost simple of type F_4, E_6^ε, E_7 or E_8 over $\mathbb{F}_q$, and let $n \geqslant 1$.*

(i) *G has at most $n^{1+o(1)}$ maximal subgroups of index n satisfying* 2.1(i, ii);

(ii) *G has at most $n^{1+27/52+o(1)}$ maximal subgroups of index n satisfying* 2.1(iii);

(iii) *G has at most $n^{1+6/11+o(1)}$ maximal subgroups of index n satisfying* 2.1(iv)–(vii).

Proof. Part (i) is clear, since there are $n^{o(1)}$ classes of maximal subgroups of type (i) and (ii), and each conjugacy class of maximal subgroups of index n contains exactly n subgroups. In the other parts the maximal subgroups M are almost simple, so it suffices to count their socles M_0 (as $M = N_G(M_0)$).

If M is as in 2.1(iii), then $|M| < c$. By [MSW, Theorem B], M_0 is generated by an involution of G_0 and another element of G_0 of order at most c. By the proof of [LiSh3, 3.5], the number of elements of G_0 of order at most c is bounded by $c_1 |G_0|^{(k-1)/k}$, where k is the dimension of the simple algebraic group of the same type as G_0. Moreover, by [LiSh2, 4.3], we have $i_2(G_0) \leqslant c_2 |G_0|^\alpha$, where $\alpha = 7/13, 20/39, 10/19, 16/31$, according as G_0 is of type F_4, E_6^ε, E_7, E_8, respectively. Therefore the number of possibilities for M_0 is at most $c_3 |G_0|^{\alpha+(k-1)/k}$, and this is at most $c_3 |G_0|^{1+27/52}$. Part (ii) follows, since $|G_0| \leqslant |G| \leqslant c|G:M| = cn$.

Now suppose M is as in 2.1(iv); then $G_0 = F_4(q)$ and $M_0 \cong A_1(q)$, $A_2^\varepsilon(q)$, $B_2^\varepsilon(q)$ or $G_2(q)$. If $N(M_0, G_0)$ denotes the number of subgroups of G_0 isomorphic to M_0, then by [LiSh3, 5.1] (as explained in the introduction of the present paper), we have

$$N(M_0, G_0) \leqslant c(i_2(G_0)\,|G_0|)/(i_2(M_0)\,|M_0|).$$

By [LiSh2, 4.1 and 4.3], we have $i_2(G_0) \sim q^{28}$, and $i_2(M_0) \sim q^2$, q^4, q^6, q^3, q^8, according as M_0 is of type A_1, A_2^ε, B_2, ${}^2B_2$, G_2, respectively; while $|G_0| \sim q^{52}$ and $|M_0| \sim q^3$, q^8, q^{10}, q^5, q^{14}, respectively. It follows that

$$N(M_0, G_0) \leqslant n^{\beta + o(1)},$$

where, for the respective possibilities for M_0, we have $\beta = 75/49$, $68/44$, $64/42$, $72/47$, $58/38$. The maximum value of β is $68/44 = 1 + 6/11$, so part (iii) follows for $G_0 = F_4(q)$. The other cases are handled in exactly the same fashion. ∎

THEOREM 2.4. *Every finite almost simple group G has at most $n^{1+6/11+o(1)}$ maximal subgroups of index n.*

Proof. If $\mathrm{soc}(G)$ is of type F_4, E_6^ε, E_7 or E_8, this follows from Proposition 2.3. For the remaining cases, the result is given by Lemmas 8–10 of [MSh]. ∎

3. Indices of Maximal Subgroups: Uniformity in p

Let $D(G)$ denote the set of degrees of faithful primitive permutation representations of a finite group G. Thus

$$D(G) = \{\,|G:M| : M \text{ max } G,\ M_G = 1\,\}.$$

Let G be an almost simple group with socle $X_k(p^a)$ of Lie type of untwisted rank k over $\mathbb{F}_{p^a}$ (where by untwisted rank, we mean the rank of the corresponding simple algebraic group). In the next result we show that, when a and k are fixed and p varies, the sets $D(G)$ change 'uniformly' with p.

THEOREM 3.1. *Given any positive integers a, k, there exist $m = m(a, k)$ and polynomials $f_1(x), \ldots, f_m(x) \in \mathbb{Q}[x]$ such that, if p is any prime, and G is an almost simple group of Lie type with socle $X_k(p^a)$, then*

$$D(G) \subseteq \{\,f_1(p), \ldots, f_m(p)\,\}.$$

Moreover, we can take $m(a, k) \leqslant ca^2k^3 \log^2 k$ and $\deg(f_i) \leqslant 4ak^2$ for all i.

Proof. Note first that given a Lie type X_k of simple groups of rank k, and a positive integer a, there is a monic polynomial $f_{X_k,\,a}(x) \in \mathbb{Z}[x]$ of degree at most $4ak^2$ such that $|X_k(p^a)| = (1/d) f_{X_k,\,a}(p)$ for all primes p for which $X_k(p^a)$ exists, where $d \in \mathbb{Z}$ and $1 \leqslant d \leqslant k+1$ (see [KL, p. 170]). Note also that $|\mathrm{Out}(X_k(p^a))| = O(ak)$.

Suppose first that G is almost simple with socle G_0 of type F_4, E_6^ε, E_7 or E_8. For maximal subgroups M satisfying 2.1(ii)–(vii), the index $|G: M| = |G_0: M \cap G_0|$ is one of at most $c.d(a)$ polynomials in p with rational coefficients, giving the conclusion in these cases (that these are polynomials rather than just rational functions is clear from the given structure of M: in 2.1(ii), observe that if $b \mid a$ then $|X_k(p^a): X_k(p^{a/b})|$ is a polynomial in p, while in (iv)–(vii), $|G_0: M_0|$ is clearly polynomial, and $|G_0: M \cap G_0| = |G_0: M_0|/e$ for some e dividing $|\mathrm{Out}(M_0)|$). From the proof of 2.1, the subgroups M under (i) of 2.1 occur either in the conclusion of [LSe1, Theorem 2], or as fixed point groups (under a Frobenius morphism) of subgroups in the conclusion of [LSe1, Theorem 1]. It follows that all subgroups M under (i) satisfy one of the following conditions:

(1) M is parabolic;

(2) $|M \cap G_0|$ is bounded;

(3) $M \cap G_0$ contains a subgroup $M(q)$ of bounded index, such that $M(q)$ is a commuting product of groups of Lie type over $\mathbb{F}_q$ and a torus (usually the torus is trivial); moreover, $|G_0: M(q)|$ is a polynomial in q with bounded rational coefficients.

The conclusion follows for subgroups M under 2.1(i).

For exceptional groups G not of type F_4, E_6^ε, E_7 or E_8, the result follows from the known lists of maximal subgroups of G in [Co, Kl1, Kl2, Ma, Su].

Assume now that $\mathrm{soc}(G) = X_k(p^a)$ is classical. Write $G_0 = \mathrm{soc}(G)$ and $q = p^a$. Let $V = V_n(q^u)$ be the natural module for G_0 (where $u = 2$ if G is unitary, $u = 1$ otherwise). Note that $n \leqslant 2k+1$. If $G_0 = D_4(q)$ then the maximal subgroups of G are determined in [Kl3]. Otherwise, the main theorem of [As] provides eight classes $\mathscr{C}_i$ $(1 \leqslant i \leqslant 8)$ of subgroups of G, such that for every maximal subgroup M of G, either

(a) $M \in \mathscr{C}_i$ for some i, or

(b) $M_0 = \mathrm{soc}(M)$ is a simple group, such that the (projective) representation of M_0 on V is absolutely irreducible and is not realised over any proper subfield of $\mathbb{F}_{q^u}$.

The conjugacy classes and structures of all subgroups in each class $\mathscr{C}_i$ are given in [KL, Chapter 4]; from this it is easily seen that $\bigcup \mathscr{C}_i$ contains less

than *cak* conjugacy classes of subgroups, and that suitable polynomials $f_1(x), ..., f_s(x) \in \mathbb{Q}[x]$ $(s \leqslant cak)$ exist, such that the conclusion holds for subgroups $M \in \bigcup \mathscr{C}_i$.

Now consider subgroups M satisfying condition (b). The smallest dimension of a nontrivial irreducible projective representation of A_m $(m \geqslant 9)$ is $m-2$ (see [KL, 5.3.7]). Hence, given n, at most cn alternating or sporadic groups have an irreducible projective representation of dimension n. Therefore, if M_0 is alternating or sporadic, then $|G:M| = |G_0: M \cap G_0|$ is one of at most cn rational polynomials in p of the form $|G_0|/e$, for suitable integers e. Thus the conclusion holds when M_0 is alternating or sporadic.

Now suppose $M_0 \cong Y_l(r)$, a group of Lie type of untwisted rank l over $\mathbb{F}_r$, and p does not divide r. By [LaSe], except for a few small groups (of bounded order), we have $n \geqslant (r^l - 1)/2$, and hence $r^l \leqslant 2n+1 \leqslant 4k+3$. In particular, $l \leqslant \log(4k+3)$. Given l, there are at most $(4k+3)^{1/l}$ choices for r; and $\sum_{1 \leqslant l \leqslant \log(4k+3)} (4k+3)^{1/l} = O(k)$. It follows that there are at most ck choices for M_0 in this case (up to isomorphism). Given M_0, the number of possibilities for $|M|$ is bounded by $|\mathrm{Out}(M_0)|$. Moreover, $|\mathrm{Out}(M_0)| \leqslant cl \log r \leqslant c' \log k$. Consequently the number of possibilities for $|M|$ (when p varies) is at most $c'' k \log k$. Thus $|G: M|$ is one of at most $c'' k \log k$ rational polynomials in p of the form $|G_0|/e$, for suitable integers e. The conclusion follows for this case.

Finally, suppose $M_0 \cong Y_l(r)$, where $p \mid r$. As in [KL, § 5.4], define $R_p(M_0)$ to be the smallest dimension of a faithful projective $\bar{\mathbb{F}}_p M_0$-module. Also, when Y_l is one of the types ${}^2A_l$, ${}^2D_l$, ${}^2E_6$ or ${}^3D_4$, let τ_0 be the restriction to M_0 of a graph automorphism of order 2, 2, 2 or 3 (respectively) of the corresponding untwisted group, and denote by $R_p^{\tau_0}(M_0)$ the smallest dimension of a faithful projective $\bar{\mathbb{F}}_p M_0$-module A such that $A \cong A^{\tau_0}$. Lower bounds for $R_p(M_0)$ and $R_p^{\tau_0}(M_0)$ are given by [KL, 5.4.8, 5.4.12, 5.4.13]. By [KL, 5.4.6 and 5.4.7], there is a positive integer v such that one of the following holds:

(i) Y_l is an untwisted type, or a Suzuki or Ree type, $r = (q^u)^v$ and $n \geqslant R_p(M_0)^v$;

(ii) Y_l is one of the types ${}^2A_l$, ${}^2D_l$, ${}^2E_6$, ${}^3D_4$, $r = (q^u)^v$ and $n \geqslant (R_p^{\tau_0}(M_0))^v$;

(iii) Y_l is one of the types ${}^2A_l$, ${}^2D_l$, ${}^2E_6$, ${}^3D_4$, $r = (q^u)^{v/a}$ (where $a = 2$, 2, 2, 3 for the respective types), and $n \geqslant (R_p(M_0))^v$.

Now $l \leqslant 2k$, by [KL, 5.2.12]. As there are at most $\log n$ choices for v, there are at most $ck \log k$ choices for M_0. It is straightforward to see that, given v and a type Y_l, in each of cases (i)–(iii) above, the index $|G:M| = |G_0: M \cap G_0| = df(q)$, where $f(x)$ is a polynomial with rational coefficients independent of q, and $d = a/b$ with a, b positive integers and $a \leqslant |\mathrm{Out}(G_0)|$,

$b \leqslant |\mathrm{Out}(M_0)|$. Moreover, $|\mathrm{Out}(G_0)| . |\mathrm{Out}(M_0)| \leqslant ca^2k^2v \leqslant c'a^2k^2 \log k$. The result follows. ∎

4. Applications to Symmetric Groups

Lemma 4.1. *Let S be a finite simple group. Then there are at most $|\mathrm{Out}(S)|^3$ almost simple groups with socle S (up to isomorphism).*

Proof. We claim that every subgroup of $\mathrm{Out}(S)$ can be generated by three elements, from which the result is immediate. When S is alternating or sporadic, $|\mathrm{Out}(S)| \leqslant 4$, so the claim is clear in these cases.

So assume now that S is of Lie type. The structure of $\mathrm{Out}(S)$ is given in [St, §§ 10, 11]. If $S \neq D_n(q)$ $(n \geqslant 4)$, then $\mathrm{Out}(S)$ has a series $1 \lhd N_1 \lhd N_2 \lhd \mathrm{Out}(S)$ with each factor group cyclic, from which the claim is obvious. And if $S = D_n(q)$ $(n \geqslant 4,\ q = p^a)$, then $\mathrm{Out}(S) \leqslant S_4 \times C_a$, and the claim follows as every subgroup of S_4 is 2-generator. ∎

Proposition 4.2. *S_n has at most $(\log n)^{9+o(1)}$ almost simple primitive subgroups up to isomorphism.*

Proof. Let $G \leqslant S_n$ be an almost simple primitive subgroup, and let $G_0 = \mathrm{soc}(G)$.

Suppose first that G_0 is a group of Lie type, say $G_0 = X_k(p^a)$. By Theorem 3.1 we have $D(G) \subseteq \{f_1(p), ..., f_m(p)\}$ where $m \leqslant ca^2k^3 \log^2 k$. Since $n \in D(G)$ there exists $i \leqslant m$ such that $n = f_i(p)$. Now, each equation $f_i(x) = n$ has at most $\deg f_i \leqslant 4ak^2$ roots. So given k, a there are at most $4ak^2m \leqslant c'a^3k^5 \log^2 k$ choices for p.

Now, the minimal degree of a nontrivial permutation representation of G_0 is at least cp^{ak} (see [KL, 5.2.2 and 5.3.9]), so $n \geqslant cp^{ak}$ and $ak \leqslant \log n$ (up to a constant, which can be ignored). Hence the number of choices for (a, k, p) is bounded by

$$\sum_{ak \leqslant \log n} c'a^3k^5 \log^2 k \leqslant \sum_{ak \leqslant \log n} c'(\log n)^5 (\log \log n)^2$$

$$\leqslant \sum_{ak \leqslant \log n} c'(\log n)^{5+o(1)}.$$

In order to bound the right hand side, note that $b := ak$ can be chosen in $\log n$ ways, and given b there are $d(b) = b^{o(1)} = (\log n)^{o(1)}$ possibilities for a, k. The number of summands on the right hand side is therefore bounded above by $(\log n)^{1+o(1)}$, and so

$$\sum_{ak \leqslant \log n} (\log n)^{5+o(1)} \leqslant (\log n)^{6+o(1)}.$$

It follows that the number of possibilities for G_0 is at most $(\log n)^{6+o(1)}$; and given G_0, the number of choices for G is at most $|\mathrm{Out}(G_0)|^3$, by Lemma 4.1. Since $|\mathrm{Out}(X_k(p^a))| \leqslant cak \leqslant c \log n$, the result follows in this case.

Now suppose $G_0 = A_k$ for some k. Let $H < A_k$ be a point-stabilizer in the action of $G_0 = A_k$ on $\{1, ..., n\}$. If H is intransitive then $n = \binom{k}{l}$ for some $l \leqslant k/2$, and there are at most $\log n$ choices for (k, l) (as $l \leqslant \log n$ and l determines k). So suppose H is transitive. Then $n = |A_k : H| \geqslant 2^{k/2}$ (see [Wi, 14.2]), so $k \leqslant 2\log n$. Altogether we see that there are at most $3 \log n$ choices for k, hence for G_0, in this case and the proof is complete. ∎

COROLARY 4.3. *S_n has at most $n^{6/11+o(1)}$ conjugacy classes of primitive almost simple subgroups.*

Proof. Let $G \leqslant S_n$ be such a subgroup. By Proposition 4.2, the isomorphism type of G can be chosen in $n^{o(1)}$ ways. Now fix an isomorphism type for G. By Theorem 2.4, G has at most $n^{6/11+o(1)}$ conjugacy classes of maximal subgroups, and this bounds the number of S_n-conjugacy classes of primitive subgroups isomorphic to G in S_n. The result follows. ∎

We can now prove the main result of this paper.

THEOREM 4.4 *S_n has at most $n^{6/11+o(1)}$ conjugacy classes of primitive maximal subgroups.*

Proof. Let $G \leqslant S_n$ be such a subgroup. We apply the O'Nan-Scott theorem in the version [KL, p. 6], according to which all primitive maximal subgroups of S_n are of affine type, diagonal type, product type or almost simple type.

First, it is clear that there is at most one class of affine type maximal subgroups, since such a subgroup is the normalizer in S_n of an elementary abelian group in its regular action.

Diagonal type maximal subgroups are of the form $N_{S_n}(T^k)$, where T is a simple group, $k \geqslant 2$ and T^k is acting on the cosets of a diagonal subgroup isomorphic to T (so $n = |T|^{k-1}$). Moreover, different choices of diagonal subgroup give conjugate subgroups T^k of S_n (see [LPS, p. 393]); hence the number of conjugacy classes of diagonal type maximal subgroups of S_n is at most the number of pairs (T, k), where T is simple and $n = |T|^{k-1}$. We claim that this number is at most 2: for if (S, l) is another such pair, then $|T|^{k-1} = |S|^{l-1}$, and hence by [KLST, 6.1], $|T| = |S|$ and $k = l$; and also by [KLST, 5.1], up to isomorphism the number of simple groups of a given order is at most 2.

Maximal subgroups of product type are of the form $G = S_k \wr S_l$ in the product action (so $n = k^l$); there are at most $\log n$ choices for G up to conjugacy.

The remaining maximal subgroups are almost simple, and these are dealt with in the previous result. ∎

Since S_n has $d(n) - 2 = n^{o(1)}$ conjugacy classes of transitive imprimitive maximal subgroups, it follows that the number of classes of transitive maximal subgroups of S_n is also bounded above by $n^{6/11 + o(1)}$.

COROLLARY 4.5. *S_n has at most $[n/2] + n^{6/11 + o(1)}$ conjugacy classes of maximal subgroups. In particular, the number of conjugacy classes of maximal subgroups of S_n is of the form $(1/2 + o(1))n$.*

Proof. This follows from the preceding remark and the fact that S_n has $[n/2]$ conjugacy classes of intransitive maximal subgroups. ∎

We conclude the paper with another consequence of Theorem 4.4.

COROLLARY 4.6. *S_n has at most $n!\, n^{-5/11 + o(1)}$ maximal subgroups. In particular, if n is large, then the number of maximal subgroups of S_n is strictly less than $n!$.*

Proof. Clearly, S_n has 2^{n-1} intransitive maximal subgroups, so it remains to count the transitive maximal subgroups. By the remark following Theorem 4.4, these subgroups split into at most $n^{6/11 + o(1)}$ conjugacy classes. Clearly, each transitive maximal subgroup of S_n has order at least n, and so it has no more than $(n-1)!$ conjugates. We conclude that S_n has at most $(n-1)!\, n^{6/11 + o(1)}$ transitive maximal subgroups. The result follows. ∎

ACKNOWLEDGMENT

The second author thanks the department of mathematics of the University of Chicago for its support and hospitality while this work was carried out.

REFERENCES

[As] M. ASCHBACHER, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514.

[B] L. BABAI, The probability of generating the symmetric group, *J. Combin. Theory Ser. A* **52** (1989), 148–153.

[Co] B. N. COOPERSTEIN, Maximal subgroups of $G_2(2^n)$, *J. Algebra* **70** (1981), 23–36.

[GL] D. GORENSTEIN AND R. LYONS, The local structure of finite groups of characteristic 2 type, *Mem. Amer. Math. Soc.* **42**, (276) (1983).

[HW] G. H. HARDY AND E. M. WRIGHT, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, Oxford, 1979.

[KLST] W. Kimmerle, R. Lyons, R. Sandling and D. N. Teague, Composition factors from the group ring and Artin's theorem on orders of simple groups, *Proc. London Math. Soc.* **60** (1990), 89–122.

[Kl1] P. B. Kleidman, The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups, *J. Algebra* **115** (1988), 182–199.

[Kl2] P. B. Kleidman, The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, of the Ree groups ${}^2G_2(q)$, and of their automorphism groups, *J. Algebra* **117** (1988), 30–71.

[Kl3] P. B. Kleidman, The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups, *J. Algebra* **110** (1987), 173–242.

[KL] P. B. Kleidman and M. W. Liebeck, The subgroup structure of the finite classical groups, London Math. Soc. Lecture Note Ser., Vol. 129, Cambridge Univ. Press, UK, 1990.

[LaSe] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418–443.

[LSe1] M. W. Liebeck and G. M. Seitz, Maximal subgroups of exceptional groups of Lie type, finite and algebraic, *Geom. Dedicata* **36** (1990), 353–387.

[LSe2] M. W. Liebeck and G. M. Seitz, Finite subgroups of exceptional groups of Lie type, to appear.

[LiSh1] M. W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata* **56** (1995), 103–113.

[LiSh2] M. W. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the (2, 3)-generation problem, *Ann. of Math.*, to appear.

[LiSh3] M. W. Liebeck and A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky, *J. Algebra*, to appear.

[LPS] M. W. Liebeck, C.E. Praeger and J. Saxl, On the O'Nan-Scott theorem for primitive permutation groups, *J. Austral. Math. Soc.* **44** (1988), 389–396.

[Ma] G. Malle, The maximal subgroups of ${}^2F_4(q^2)$, *J. Algebra* **139** (1991), 52–69.

[MSW] G. Malle, J. Saxl, and T. Weigel, Generation of classical groups, *Geom. Dedicata* **49** (1994), 85–116.

[MSh] A. Mann and A. Shalev, Simple groups, maximal subgroups, and probabilistic aspects of profinite groups, *Israel J. Math.*, to appear.

[P] L. Pyber, Asymptotic results for permutation groups, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science* **11** (1993), 197–219.

[PSh1] L. Pyber and A. Shalev, Groups with super-exponential subgroup growth, *Combinatorica*, to appear.

[PSh2] L. Pyber and A. Shalev, Asymptotic results for primitive permutation groups and some applications, in preparation.

[St] R. Steinberg, Lecture on Chevalley groups, Yale University Lecture Notes, 1968.

[Su] M. Suzuki, On a class of doubly transitive groups, *Ann. of Math.* **75** (1962), 105–145.

[Wa] G. E. Wall, Some applications of the Eulerian function of a finite group, *J. Austral. Math. Soc.* **2** (1961), 35–59.

[Wi] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.